ИНФОРМАЦИОННАЯ СИСТЕМА КОНТРОЛЯ РАБОТЫ СМЕННЫХ НОСИТЕЛЕЙ КОМПЬЮТЕРНОЙ СЕТИ УЧЕБНОГО ЗАВЕДЕНИЯ

И.М. Удовик, О.О. Байбуз
(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

Для защиты и администрирования компьютерной сети учебного заведения важно предотвратить запись информации на сменные носители и установку с них ненужных программ. При помощи автоматизированной системы контроля сменных носителей администратор компьютера или домена может контролировать доступ пользователей к дисководам, DVD/CD-ROM'ам, другим сменным устройствам, адаптерам WiFi и Bluetooth, а также к USB, FireWire, инфракрасным, COM и LPT-портам.

Кроме функции контроля доступа, автоматизированная система контроля сменных носителей осуществляет протоколирование и аудит использования устройств на локальном компьютере как отдельными пользователями, так и группами. Для хранения записей аудита система использует стандартный журнал Windows, что позволит просматривать их как с помощью стандартной программы просмотра событий, так и встроенного средства.

DeviceLock состоит из трех частей:

- агента (DeviceLockService)
- сервера (DeviceLockEnterprise Server)
- консоли управления (DeviceLock Management Console, DeviceLock Group Policy Manager и DeviceLock Enterprise Manager).

DeviceLockService – это ядро системы StoregeWall. Агент устанавливается на каждый компьютер, автоматически запускается и обеспечивает защиту устройств на машине-клиенте, оставаясь в то же время невидимым для локального пользователя. Структура ядра системы DeviceLock дана на рис. 1.

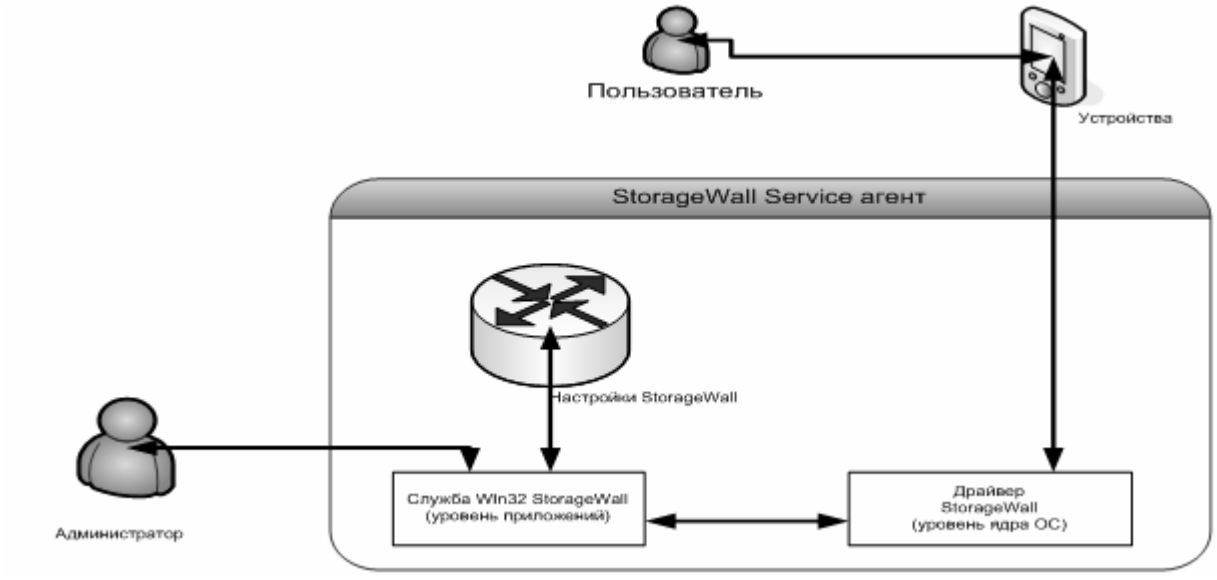

Рис. 1. Структура ядра системы.

DeviceLock Enterprise Server – это дополнительный необязательный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита [1]. DeviceLock Enterprise Server использует MS SQL Server для хранения данных. Вы можете установить несколько экземпляров DeviceLock Enterprise Server в вашей сети, чтобы равномерно распределить нагрузку.

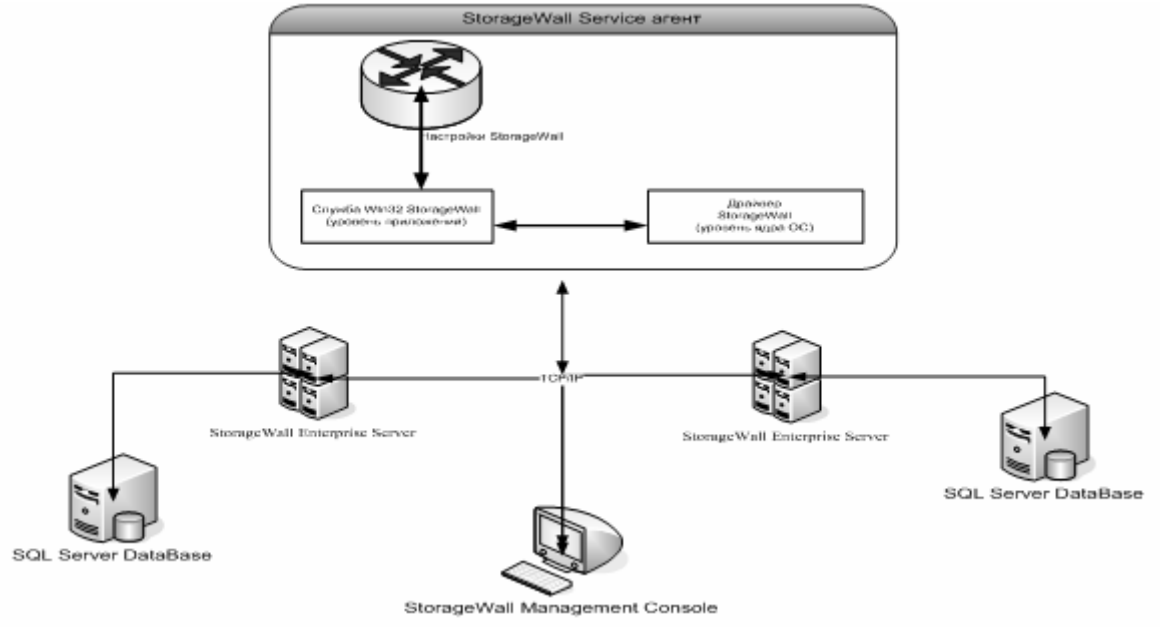

Рис. 2. Структура DeviceLock Enterprise Server .

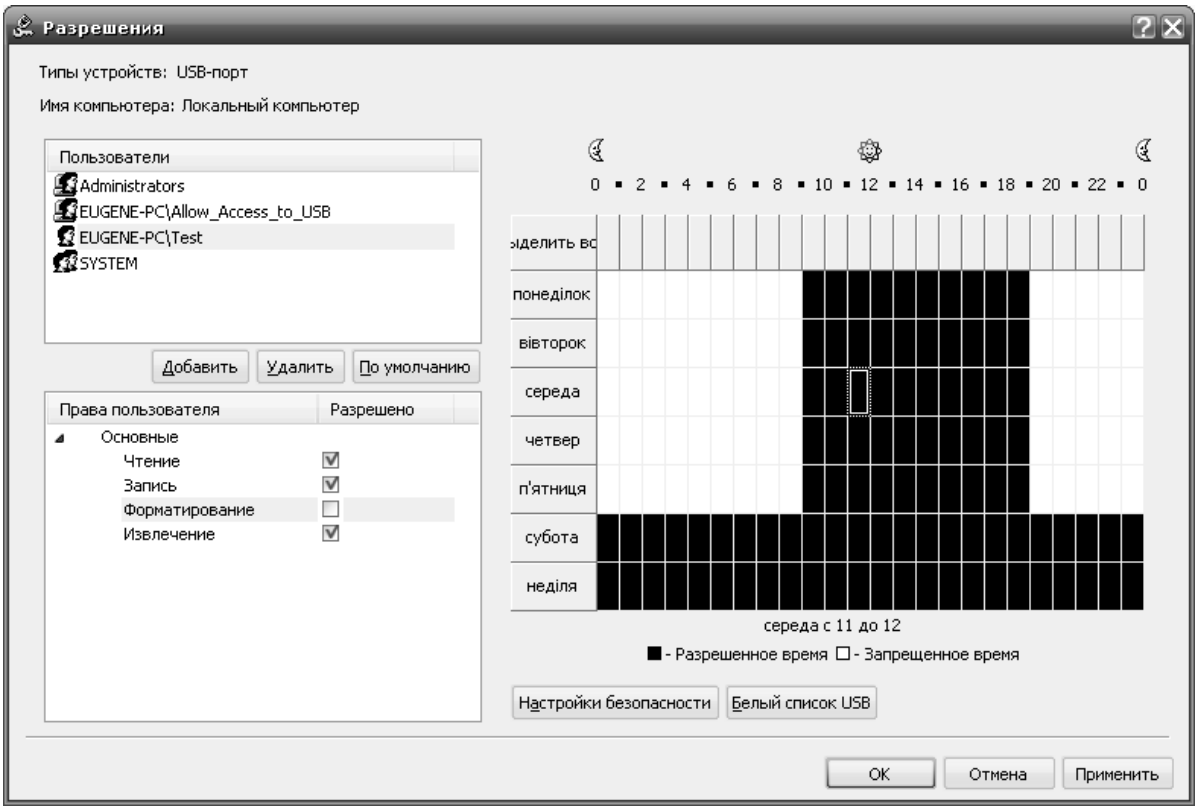

Рис. 3. Пример создания конфигурации usb устройства.

Консоль управления – это интерфейс контроля, который системный администратор использует для удаленного управления любой системой, на которой установлен агент (DeviceLock Service). DeviceLock разработан с тремя различными консолями управления: DeviceLock Management Console (оснастка для MMC), DeviceLock Enterprise Manager и DeviceLock Group Policy Manager (интегрирован в редактор групповых политик Windows). DeviceLock Management Console также используется для управления DeviceLock Enterprise Server'ом.

Автоматизированная система для контроля сменных носителей учащихся, была написана с использованием технологии MFC [2] в интегрированной среде разработки Microsoft Visual Studio 2008.

Пример создания конфигурации usb устройства, для пользователя с учетной записью Test, представлен на рис. 3.

Возможности по управлению внешними устройствами, имеющиеся в современных операционных системах, реализуют, как правило, только базовый функционал разграничения доступа и не обеспечивают необходимой гибкости, безопасности и расширенных функций. Таким образом, только специализированные системы контроля доступа к внешним устройствам могут обеспечить приемлемый уровень снижения риска утечек информации.

Список литературы

1. http://ic-dv.ru/catalog/nsd/devicelock/
2. А.Мешков, Ю.Тихомиров. Visual C++ и MFC. 2-е изд.перераб. и доп. – СПб.: БХВ-Петербург, 2003. – 1040стр.

МОДЕЛИРОВАНИЕ УСТРОЙСТВА КОДИРОВАНИЯ РЕЧЕВОГО СИГНАЛА

О.М. Галушко, Массембо Элика Селесте
(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

Известно, что наиболее надежными методами защиты от прослушивания речевой информации являются криптографические методы:

- преобразование аналоговых параметров речи;
- цифровое шифрование.

Устройства, использующие эти методы, называются скремблерами.

При **аналоговом** скремблировании производится изменение характеристики исходного звукового сигнала таким образом, что результирующий сигнал становится неразборчивым, но занимает ту же частотную полосу. Это дает возможность без проблем передавать его по обычным каналам связи. При этом методе сигнал может подвергаться следующим преобразованиям:

- частотная инверсия;
- частотная перестановка;
- временная перестановка.